REMARKS

The Examiner is thanked for the performance of a thorough search. By this amendment, Claim 12 has been amended. Claims 40–48 have been added. Claims 14–22 are canceled. Hence, Claims 1, 3–13, 23–25, 27–32, and 34–48 are pending in this application.

All issues raised in the Office Action are addressed hereinafter.

I.   ADDED CLAIMS / AMENDMENTS

The added claims and amendments to the claims do not add new matter to this application. The amendment to Claim 12 addresses informalities, so as to put Claim 12 in condition for allowance.

Claims 40–48 have been added. Claims 40–48 correspond to claims 3-11 but are recited in computer-readable storage medium format. Thus, claims 40-48 do not introduce any new subject matter. Furthermore, Claims 40–48 are patentable over the cited references for the same reasons as explained for Claim 23, from which Claims 40–48 depend.

II.   CLAIM REJECTIONS BASED ON 35 U.S.C. § 103

A.   *Claims 1, 3, 6–8, 10–13, 23–25, 27, 30–32, 34, and 37–39: Sharma, Daude and Garrett.*

Claims 1, 3, 6–8, 10–13, 23–25, 27, 30–32, 34, and 37–39 were rejected under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 6,754,716 (hereinafter "*Sharma*") in view of U.S. Patent No. 7,231,660 B1 to Daude, et al. (hereinafter "*Daude*") and further in view of Garrett et al (hereinafter "*Garrett*") U.S. Pub. No. 2002/0023174 A1. Applicants traverse the rejection. Reconsideration is respectfully requested.

CLAIM 1

Claim 1, as set forth in the listing of claims, clarifies that the method features, among other elements:

receiving an instruction to update an ARP table from a particular
subsystem of a network device;
determining whether the particular subsystem within the network
device from which the instruction originated is authorized;
wherein determining that the particular subsystem is
authorized comprises **determining that the
particular subsystem _is_ a** Dynamic Host
Configuration Protocol (DHCP) server, an
Authentication, Authorization, Accounting (AAA)
server or a Network Address Translator (NAT); and
only if the particular subsystem is authorized, then updating the
ARP table based on the instruction.

Sharma, by contrast, describes determining that a network device is authorized by determining whether or not the IP address of the network device is in "a list of authorized IP addresses," *Sharma* at col. 3, lines 12–16, and col. 5, lines 20–33, or by determining whether or not its "protocol and L2 [MAC] address . . . form an authorized address pair," *Sharma* at col. 7 lines 10–15. In other words, *Sharma* describes making an authorization determination based on only the IP address and the MAC address.

By further contrast, *Daude* describes preventing unauthorized DHCP servers from responding to DHCP requests. *Daude* detects unauthorized DHCP servers by "comparing a 'server identifier' option included in the DHCPOFFER message returned by the HDCP servers ... with authorized server identification data in DHCP server table 206." *Daude* at col. 9, lines 25–28. *Daude* describes that if an IP address in the server identifier is in a list of authorized DHCP server addresses, the corresponding DHCP server is authorized. *See Daude* at col. 11, lines 3–13. *Daude* only discusses DHCP, and is not related to ARP.

Finally, *Garrett* describes and approach that can, for address assignment via DHCP, "restrict address assignment to authorized hosts and to prevent clients from accepting addresses from invalid DHCP servers." *Garrett* at ¶ [0035]. To achieve this goal, *Garrett* describes authorization via "delayed authentication" or Kerberos. *Id.* The former technique relies on "a shared secret." *Id.* The latter technique relies on "realms." *Id. Garrett* also describes to "restrict access to . . . network access devices that are properly registered and authenticated." *Garrett* at ¶ [0038]. *Garrett* achieves this goal by relying on a CMTS 225 to "snoop" DHCPACK messages for IP addresses and MAC addresses, which are stored in the "yiaddr" and

"chaddr" fields. *See* FIG. 11 and ¶ [0039]. Based on this information, CMTS 225 "populate[s] its ARP cache." *Garrett* at ¶ [0038]. Significantly, *Garrett* describes that CMTS should populate its ARP cache "without resorting to broadcasting an ARP request." *Id.* Since DHCPACK messages are only sent to a device if the device is authorized, populating CMTS 225's ARP cache by snooping DHCPACK messages instead of sending ARP requests ensures that devices in the ARP cache are properly registered. *Id.*

Thus, the combination of *Sharma*, *Daude*, and *Garrett* fails to teach or suggest a number of features of Claim 1.

(1) The references do not disclose determining that a device is authorized based on what the device is.

Claim 1 recites "determining that the particular subsystem is authorized comprises **determining that the particular subsystem *is* a** Dynamic Host Configuration Protocol (DHCP) server, an Authentication, Authorization, Accounting (AAA) server or a Network Address Translator (NAT)." In other words, for purposes of determining whether or not to update an ARP table in response to an ARP request, Claim 1 recites to determine **what type of device** requested the update. Specifically, a requesting subsystem is determined to be authorized only if it is determined to be one of the following types of devices: a DHCP server, AAA Server, or NAT.

By contrast, the cited references neither teach nor suggest "determining that the particular subsystem is a Dynamic Host Configuration Protocol (DHCP) server, an Authentication, Authorization, Accounting (AAA) server or a Network Address Translator (NAT)." Nonetheless, the Office Action alleges that *Garrett* teaches such a step in FIG. 11, steps 1101, 1102, and 1103, along with ¶¶ [0035], [0038], and [0039]. The Office Action is clearly in error.

Except ¶ [0035], none of these passages deals with an authorization determination of any type. With regards to ¶ [0035], *Garrett* very clearly explains that the authorization determination is performed by "delayed authentication" or "Kerberos." Neither of these technologies relies on determining the **type of a subsystem**. Should the Office persist in its rejection on the basis of *Garrett*, ¶ [0035], Applicants respectfully request that the Office clearly explain how *Garrett*'s disclosure of "delayed authentication" or "Kerberos" constitutes "**determining that a particular**

subsystem _is_ a Dynamic Host Configuration Protocol (DHCP) server, an Authentication, Authorization, Accounting (AAA) server or a Network Address Translator (NAT)."

With regards to the other cited passages, _Garrett_, at FIG. 1101, 1102, and 1103, and ¶¶ [0038]—[0039] shows how _Garrett_'s CMTS 225 may update an ARP table based upon information snooped from a DHCPACK message, which is sent only after authentication through the processes explained in ¶ [0035]. As shown in step 1103, the ARP table is updated unconditionally in response to intercepting the DHCPACK message. _Garrett_ features no step of intermediary step of determining whether or not a device is authorized between receiving the DHCPACK and updating an ARP table.

Thus, neither the cited passages nor any other passage in _Garrett_ teaches a step of "determining that [a] particular subsystem is authorized" by "determining that the particular subsystem is a [particular type of device]."

This element is also missing from _Sharma_ and _Daude_. Applicants have previously explained why _Sharma_ and _Daude_ fail to teach or suggest such an element. Accordingly, the Office Action acknowledges that _Sharma_ or _Daude_ does not teach this element.

(2) Garrett is incompatible with Sharma

Even if _Garrett_ taught a step of "determining that [a] particular subsystem is authorized" by "determining that the particular subsystem is a [particular type of device]," one skilled in the art could not have combined _Sharma_ and _Garrett_. Therefore, _Sharma_ in view of _Garrett_ would not have taught one skilled in the art the method of Claim 1.

Garrett's CMTS 225 never receives an ARP update request. Rather, _Garrett_'s CMTS 225 always updates the ARP cache when it sees a DHCPACK message, without performing any additional step of authorization. The CMTS 225 simply assumes that if it sees a DHCPACK message, the device to whom the DHCPACK is sent has already been authorized. _See Garrett_ at ¶¶ [0038] and [0039]. In fact, _Garrett_ **teaches away** from receiving an ARP update request in ¶ [0038], which explains that the ARP cache is updated "without resorting to broadcasting an ARP request." _Sharma_, on the other hand, specifically describes updating the ARP table upon receiving an ARP update request from an authorized client. _See Sharma_ at col. 3, lines 12–23. The two techniques for updating the ARP table are incompatible. For instance, if _Garrett_'s

CMTS 225 were also to modify its ARP cache based on ARP update requests, as taught by *Sharma*, *Garrett* would be unable to ensure that the sender of the message had been authorized through Kerberos or delayed authentication. Thus, the combination of *Sharma* and *Garrett* is inoperative.

For at least the foregoing reasons, the combination of *Sharma*, *Daude*, and *Garrett* fails to teach or suggest at least one feature of independent Claim 1. Therefore, the combination of *Sharma*, *Daude*, and *Garrett* does not render Claim 1 obvious under 35 U.S.C. § 103. Reconsideration is respectfully requested.

CLAIM 12

Claim 12, as set forth in the listing of claims, clarifies that the method features, among other elements:

> ***if*** **the particular network interface is contained in the set of one**
> **or more specified network interfaces**, or **if the particular**
> **network address is contained in the set of one or more**
> **specified network addresses**, ***then*** **performing** steps
> comprising:
> determining whether a particular subsystem in a network element
> from which the instruction originated is authorized;
> wherein determining that the particular subsystem is
> authorized comprises **determining that the**
> **particular subsystem *is* a** Dynamic Host
> Configuration Protocol (DHCP) server, an
> Authentication, Authorization, Accounting (AAA)
> server or a Network Address Translator (NAT);
> only if the particular subsystem is authorized, then updating the
> ARP table based on the instruction; and

The combination of *Sharma*, *Daude*, and *Garrett* fails to teach or suggest a number of features of Claim 1.

> *(1) The references do not disclose determining that a device is authorized based on what the device is.*

Like Claim 1, Claim 12 explicitly requires "determining that the particular subsystem is authorized comprises **determining that the particular subsystem *is* a** Dynamic Host

Configuration Protocol (DHCP) server, an Authentication, Authorization, Accounting (AAA) server or a Network Address Translator (NAT)." As explained with regards to Claim 1, the combination of *Sharma*, *Daude*, and *Garrett* discloses no such feature.

(2) *Garrett is incompatible with Sharma*

Furthermore, as explained with regards to Claim 1, the combination of *Sharma* and *Garrett* is inoperative. One skilled in the art could not have combined *Sharma* and *Garrett*. Therefore, *Sharma* in view of *Garrett* would not have taught one skilled in the art the method of Claim 12.

(3) *The references do not disclose determining if a device is authorized, **only if** the device's address is in a certain set of address*

Claim 12 recites that "determining whether a particular subsystem in a network element from which the instruction originated is authorized" occurs **only after first checking if** the network device has a "network interface [that] is contained in the set of one or more specified network interfaces, or [a] particular network address [that] is contained in the set of one or more specified network addresses." In other words, Claim 12 performs its step of authorization only if a device's network address or MAC address is in a certain range of addresses.

By contrast, the cited references neither teach nor suggest such a technique. The Office Action alleges that *Sharma* teaches such a technique in *Sharma* at FIG. 6, step 604, and col. 3, lines 12–34. The Office Action is clearly in error.

Sharma at FIG. 6, step 604, and col. 3, lines 12–34, both describe to check if a "host is authorized to request an L2 address." However, this step is not accomplished **after** checking if the host's network address is in a set of addresses or if the host's MAC address is in a set of MAC addresses. Rather, this step is accomplished **by** checking if the host's network address is in a set of addresses or if the host's MAC address is in a set of MAC addresses. *See* col. 3 at lines 16–17; col. 7, lines 9–10. Thus, Sharma's authorization step occurs unconditionally. This technique is clearly different from Claim 12's technique of performing authorization only in certain conditions.

Furthermore, the Office Action relies upon the exact same step 604 for teaching Claim 12's step of "determining whether a particular subsystem . . . is authorized" as it did for teaching Claim 12's step "determining whether a particular network address . . . is contained in a set of one or more specified network addresses." The Office Action is clearly in error, since Claim 12's step of "determining whether a particular subsystem . . . is authorized" is clearly a separate step that must occur after the "determining whether a particular network address . . . is contained in a set of one or more specified network addresses." *Sharma*'s step 604 cannot teach both steps.

In other words, according to the Office Action's analysis, *Sharma* would teach one to perform step 604 of *Sharma* and then, if network address is in a set of authorized network addresses, to redundantly perform step 604 again. Yet, no such behavior is described in *Sharma*. Nor would *Sharma* teach such behavior because one would not, after determining that a device is authorized in step 604, subsequently have need of repeating this authorization step again. The Office Action's analysis, then, must be in error.

This element is also missing from *Daude* and *Garrett*. In fact, the Office Action did not rely upon *Daude* or *Garrett* for teaching or suggesting this element.

For at least the foregoing reason, the combination of *Sharma*, *Daude*, and *Garrett* fails to teach or suggest at least one feature of independent Claim 12. Therefore, the combination of *Sharma*, *Daude*, and *Garrett* does not render Claim 12 obvious under 35 U.S.C. § 103. Reconsideration is respectfully requested.

CLAIMS 23–25

Independent Claims 23–25 also recite features argued above with relation to Claim 1, although Claim 1 is expressed in another format. Because each of Claims 23–25 has at least one of the features described above for Claim 1, Claims 23–25 are therefore allowable over the combination of *Sharma*, *Daude*, and *Garrett* for at least one of the same reasons as given above for Claim 1. Reconsideration is respectfully requested.

CLAIMS 3, 6–8, 10–11, 13, 27, 30–32, 34, AND 37–39

Each of Claims 3, 6–8, 10–11, 13, 27, 30–32, 34, and 37–39 depends from one of Claims 1, 12, or 24–25, and includes the above-quoted features of its parent claim by dependency. Thus,

the combination of *Sharma*, *Daude*, and *Garrett* also fails to teach or suggest at least one feature found in Claims 3, 6–8, 10–11, 13, 27, 30–32, 34, and 37–39. Therefore, the combination of *Sharma*, *Daude*, and *Garrett* does not render obvious Claims 3, 6–8, 10–11, 13, 27, 30–32, 34, and 37–39. Reconsideration of the rejection is respectfully requested.

In addition, each of Claims 3, 6–8, 10–11, 13, 27, 30–32, 34, and 37–39 recites at least one feature that independently renders it patentable. For example, **Claim 7** recites:

> **if the particular subsystem is not authorized**, then performing
>> the steps of:
>> determining **whether a particular network interface**
>>> through which the instruction was received **is
>>> contained in a set of one or more specified
>>> network interfaces**

The Office Action alleges that *Sharma* teaches such a step in *Sharma*, FIG. 5, step 502. The Office Action is in clear error. In *Sharma*, step 502, *Sharma* disclose determining if a device is authorized. **If a device is not authorized**, *Sharma* explicitly states that, in step 504, the **ARP request is discarded**. Clearly, then, *Sharma* does not teach "determining whether a particular network interface through which the instruction was received is contained in a set of one or more specified network interfaces" if the device is not authorized.

As another example, **Claim 8** recites:

> **if the particular subsystem is not authorized**, then performing
>> the steps of:
>> determining **whether a particular network address** indicated by
>>> the instruction **is contained in a set of one or more
>>> specified network addresses**;

The Office Action alleges that *Sharma* teaches such a step in *Sharma*, FIG. 5, step 502. The Office Action is in clear error. In *Sharma*, step 502, *Sharma* disclose determining if a device is authorized. **If a device is not authorized**, *Sharma* explicitly states that, in step 504, the **ARP request is discarded**. Clearly, then, *Sharma* does not teach "determining whether a particular network address indicated by the instruction is contained in a set of one or more specified network addresses" if the device is not authorized.

As another example, **Claim 10** features the limitation that "the ARP table is updated **only in response to instructions that are not ARP messages**." *Sharma* does not contemplate ignoring all ARP messages. In fact, *Sharma* appears to contemplate that ARP updates occur only in response to ARP messages. The Office Action alleges that *Sharma* discloses this feature in col. 3, lines 6–34. However, this passage of Sharma discloses that, while some ARP messages may indeed be ignored, authorized ARP messages are still used to update the ARP table. Thus, *Sharma* does not disclose that "the ARP table is updated only in response to instructions that are not ARP messages."

To expedite prosecution in light of the fundamental differences already identified, further arguments for each independently patentable feature of Claims 3, 6–8, 10–11, 13, 27, 30–32, 34, and 37–39 are not provided at this time. Applicants reserve the right to further point out the differences between the cited art and the novel features recited in the dependent claims.

B.   *Claims 4-5, 28-29, and 35-36: Sharma, Daude, Garrett and Wilson.*

Claims 4–5, 28–29, and 35–36 are rejected under 35 U.S.C. § 103(a) as being unpatentable over *Sharma* in view of *Daude, Garrett* and further in view of *Wilson*. Applicants traverse the rejection. Reconsideration is respectfully requested.

Each of Claims 4–5, 28–29, and 35–36 depends from one of Claims 1, 24, or 25, and includes the above-quoted features of its parent claim by dependency. Thus, the combination of *Sharma, Daude, Garrett*, and *Wilson* also fails to teach or suggest at least one feature found in Claims 4–5, 28–29, and 35–36. Therefore, the combination of *Sharma, Daude, Garrett*, and *Wilson* does not render obvious Claims 4–5, 28–29, and 35–36. Reconsideration of the rejection is respectfully requested.

In addition, each of Claims 4–5, 28–29, and 35–36 recites at least one feature that independently renders it patentable. However, to expedite prosecution in light of the fundamental differences already identified, further arguments for each independently patentable feature of Claims 4–5, 28–29, and 35–36 are not provided at this time. Applicants reserve the right to further point out the differences between the cited art and the novel features recited in the dependent claims.

C.   *Claim 9: Sharma, Daude, Garrett and Massarani.*

Claim 9 is rejected under 35 U.S.C. § 103(a) as being unpatentable over *Sharma* in view of *Daude* and in further view of *Garrett* (hereinafter *Garrett*) U.S. Pub. No. 2002/0023174 A1 and in further view of *Massarani*. Applicants traverse the rejection. Reconsideration is respectfully requested.

Each of Claims 4–5, 28–29, and 35–36 depends from one of Claims 1, 24, or 25, and includes the above-quoted features of its parent claim by dependency. Thus, the combination of *Sharma*, *Daude*, *Garrett*, and *Wilson* also fails to teach or suggest at least one feature found in Claims 4–5, 28–29, and 35–36. Therefore, the combination of *Sharma*, *Daude*, *Garrett*, and *Wilson* does not render obvious Claims 4–5, 28–29, and 35–36. Reconsideration of the rejection is respectfully requested.

In addition, each of Claims 4–5, 28–29, and 35–36 recites at least one feature that independently renders it patentable. However, to expedite prosecution in light of the fundamental differences already identified, further arguments for each independently patentable feature of Claims 4–5, 28–29, and 35–36 are not provided at this time. Applicants reserve the right to further point out the differences between the cited art and the novel features recited in the dependent claims.

D.   *Claims 14-22: Massarani, Chien, and Daude.*

Claims 14–22 are rejected under 35 U.S.C. § 103(a) as being unpatentable *Massarani* in view of U.S. Pub. No. 2003/0115345 to Chien et al. (hereinafter *Chien*) and further in view of *Daude*.

Although Applicants disagree with the basis of rejection for Claims 14–22, Claims 14–22 have been canceled so as to expedite consideration of the other claims and thus put the application in condition for allowance. Therefore, the rejection is now moot. Applicants reserve the right to argue Claims 14–22, or the subject matter thereof, at a later date.

III.   CONCLUSION

For the reasons set forth above, all of the pending claims are now in condition for

allowance. The Examiner is respectfully requested to contact the undersigned by telephone

relating to any issue that would advance examination of the present application.

If any applicable fee is missing or insufficient, throughout the pendency of this

application, the Commissioner is hereby authorized to any applicable fees and to credit any

overpayments to our Deposit Account No. 50-1302.

Respectfully submitted,
HICKMAN PALERMO TRUONG & BECKER LLP

Date: 5/9/08   /KarlTRees#58983/
                                                               Karl T. Rees, Reg. No. 58,983

2055 Gateway Place, Suite 550
San Jose, CA 95110
(408) 414-1233
Facsimile: (408) 414-1076